

DIALOG(R) File 351:Derwent WPI
(c) 2002 Derwent Info Ltd. All rts. reserv.

011612519 **Image available**

WPI Acc No: 1998-029647/ 199803

XRPX Acc No: N98-023887

**Encrypted software circulation method used in PC for CD-ROM - involves
decoding of encipherment part of set of software purchased by user, using
decoding program from analysis result of password analysis program**

Patent Assignee: HITACHI LTD (HITA)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 9288576	A	19971104	JP 9699815	A	19960422	199803 B

Priority Applications (No Type Date): JP 9699815 A 19960422

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 9288576	A		6 G06F-009/06	

Abstract (Basic): JP 9288576 A

The method involves performing input of a bit row of a state, where a bit corresponding to one software among software list purchased by the user, as a password to the user. A password analysis program (140) is started where the password is input.

The decoding of an encipherment part of the software purchased by user is performed using a decoding program from an analysis result of the password analysis program and purchased software are able to be used.

ADVANTAGE - Prevents inaccurate use of software not purchased.

Dwg.1/3

Title Terms: ENCRYPTION; SOFTWARE; CIRCULATE; METHOD; CD; ROM; DECODE; PART
; SET; SOFTWARE; PURCHASE; USER; DECODE; PROGRAM; ANALYSE; RESULT;
PASSWORD; ANALYSE; PROGRAM

Derwent Class: T01

International Patent Class (Main): G06F-009/06

File Segment: EPI

Manual Codes (EPI/S-X): T01-D01; T01-F06; T01-J20X

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-288576

(43) 公開日 平成9年(1997)11月4日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 Z 5 5 0 A

審査請求 未請求 請求項の数2 O L (全 6 頁)

(21) 出願番号 特願平8-99815

(22) 出願日 平成8年(1996)4月22日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 下田 英和

神奈川県横浜市中区戸塚戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者 大橋 浩幸

神奈川県横浜市中区戸塚戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人 弁理士 小川 勝男

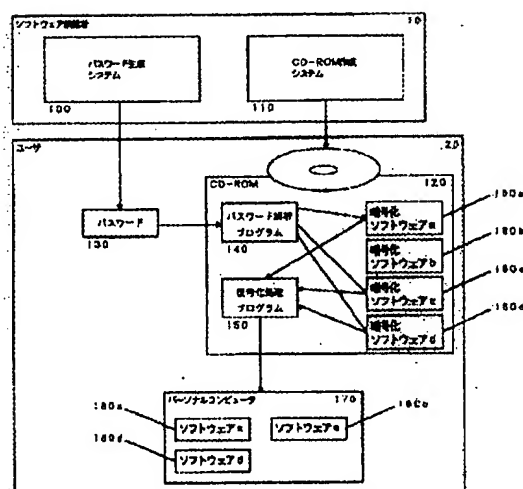
(54) 【発明の名称】 ソフトウェア配布方法

(57) 【要約】

【課題】 1つのパスワードの入力により記憶媒体に格納された複数の暗号化されたソフトウェアの暗号化部分が復号化プログラムにより復号化されユーザが購入したソフトウェアのみが使用できるようにする。

【解決手段】 配布記憶媒体に複数のコンピュータプログラムやデータなどのソフトウェアを暗号化して格納し配布する方法において、配布媒体に格納してあるソフトウェアのソフトウェアリストをビット列化したものに対しユーザが購入するソフトウェアに対応するビットを立てた状態のビット列を暗号化し文字列化したものをパスワードとしてユーザに付与し、その1つのパスワードの入力によりパスワード解析プログラムを起動させ、パスワード解析プログラムの解析結果から複数のソフトウェアの暗号化部分が復号化プログラムにより復号化されユーザが購入したソフトウェアのみが使用できるようになる。

図 1



【特許請求の範囲】

【請求項1】配布記憶媒体に複数のコンピュータプログラムやデータなどのソフトウェアを暗号化して格納し配布するソフトウェア配布方法であって、配布記憶媒体に格納してあるソフトウェアのソフトウェアリストをビット列化したものに対しユーザが購入するソフトウェアに対応するビットを立てた状態のビット列を暗号化し文字列化したものをパスワードとしてユーザに付与し、その1つのパスワードの入力によりパスワード解析プログラムが起動され、パスワード解析プログラムの解析結果から複数のソフトウェアの暗号化部分が復号化プログラムにより復号化されユーザが購入したソフトウェアのみが使用できるようになることを特徴としたソフトウェア配布方法。

【請求項2】前記パスワード解析プログラムと復号化処理プログラムとを暗号化した複数のソフトウェアとともに前記配布媒体に格納することを特徴とする請求項1記載のソフトウェア配布方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はソフトウェア配布方法に係り、特に、CD-ROMなどの大容量配布媒体にソフトウェアを暗号化し格納して配布することにより、ユーザが購入していないソフトウェアを不正に使用できないようにするソフトウェア配布方法に関するものである。

【0002】

【従来の技術】パーソナルコンピュータなどのソフトウェアはフロッピーディスクなどの比較的記憶容量が小さく比較的安価な媒体に格納して配布されていた。ソフトウェアの規模が次第に大型化し、ファイルのサイズ、数量などが増大していった。大型化したソフトウェアの配布に低容量の媒体では数十枚の媒体が必要になり、ソフトウェアベンダでの配布媒体のコストが増大し、ソフトウェアを使用するユーザ側でもソフトウェアのインストールに非常に多くの時間と手間がかかってしまっていた。

【0003】近年、音楽用コンパクトディスクの普及が目覚ましく、非常に安価なコストでコンパクトディスクが生産できるようになってきた。このコンパクトディスクをコンピュータのデータ読み出し専用の媒体としてCD-ROMが開発され、最近ではCD-ROMを読み出す装置（CD-ROMドライブ）が低価格で販売されるようになり、ほとんどのパーソナルコンピュータに接続されるようになってきている。このCD-ROMはフロッピーディスクの約500枚分の記憶容量を持ち、コンパクトディスクのプレス技術により短期間に低コストで大量生産できる利点がある。フロッピーディスクによるソフトウェアの配布よりもすべての面で優れているCD-ROMによるソフトウェアの配布が一般化しつつあ

る。

【0004】さらに最近では、複数のソフトウェアを暗号化してCD-ROMに格納し配布する方法が行われている。この方法に関連する公知例としては、特開平7-93148号公報や特開平7-182244号公報がある。

【0005】この配布方法では、ソフトウェア供給者はCD-ROMに複数のソフトウェアを暗号化して格納したり、デモ用のソフトウェアなどを暗号化せずに格納してユーザに無料もしくは低価格で配布する。利用者はデモ用のソフトウェアなどで購入する前に試しに使ってからソフトウェアの購入を決められる。ソフトウェアを購入する場合は、ソフトウェア供給者にソフトウェアの購入申請をすると、ソフトウェアに対応した暗号化されたソフトウェアを復元するためのパスワードが提供され、その場で購入したソフトウェアが使用できるようになる。このように複数のソフトウェアを安価に配布できソフトウェアの流通コストを大幅に削減できる。

【0006】

【発明が解決しようとする課題】しかし、上記の配布方法では1つのソフトウェア毎に1つのパスワードが提供されるため一度に複数のソフトウェアを購入しインストールする場合、購入したソフトウェアの数分だけ意味の無い文字列であるパスワードを入力しなければならず、単純な作業のほずであるインストール作業が非常に煩雑で面倒な作業になってしまう。

【0007】本発明は上記の問題点を解決するために1つのパスワードから配布媒体に格納されている暗号化された複数のソフトウェアを復号化しインストールできるソフトウェア配布方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するために、本発明では配布媒体に複数のコンピュータプログラムやデータなどのソフトウェアを暗号化して格納し配布するソフトウェアの配布方法において、配布媒体に格納してあるソフトウェアのソフトウェアリストをビット列化したものに対しユーザが購入するソフトウェアに対応するビットを立てた状態のビット列を暗号化し文字列化したものをパスワードとしてユーザに付与し、その1つのパスワードの入力によりパスワード解析プログラムが起動され、パスワード解析プログラムの解析結果から複数のソフトウェアの暗号化部分が復号化プログラムにより復号化されユーザが購入したソフトウェアのみが使用できるように構成した。

【0009】また、前記パスワード解析プログラムと復号化処理プログラムとを暗号化した複数のソフトウェアとともに前記配布媒体に格納するようにしている。

【0010】

【発明の実施の形態】次に本発明の一実施例を図面を用いて詳細に説明する。図1は本発明により実現されるソフトウェア配布方法を模式的に示したものである。

【0011】図1で、10はソフトウェア供給者ですなわち、ソフトウェアの開発、販売または販売のみを行うコンピュータソフトウェアベンダである。このソフトウェア供給者には、パスワード生成システム100とCD-ROM作成システム110がある。ユーザ20はパーソナルコンピュータ170を使用してソフトウェア供給者10から配布されたCD-ROM120に格納される暗号化ソフトウェア160を、パスワード130を入力することにより暗号化ソフトウェア160を利用する。

【0012】パスワード生成システム100では、ユーザ20から購入希望のあったソフトウェアの情報と配布しているCD-ROM120に関する情報（シリアルNo. など）とCD-ROM120に格納してあるソフトウェアリストの情報などを元にして、ユーザ20に提供するパスワード130を生成する。生成したパスワード130は、郵送、FAX、電子メールなどの手段でユーザ20に提供する。

【0013】CD-ROM作成システム110では、ユーザ20に提供するCD-ROMの原盤を作成する。この原盤はCD-Rで作成し、このCD-RをCD-ROMプレス会社にプレス依頼することにより大量のCD-ROM120を短時間に低コストで生産することができる。

【0014】ユーザ20に提供するCD-ROM120には、暗号化してあるソフトウェア160、パスワード解析プログラム140、復号化処理プログラム150などを格納している。

【0015】160a、160b、160c、160dの暗号化ソフトウェア160は、従来の配布方法ではそれぞれのソフトウェアを暗号化せずに販売や配布の単位となっていたものである。また、CD-ROM120には機密の保護や料金の徴収の必要無いデモ版や体験版のソフトウェアを暗号化しないでCD-ROM120に格納して配布してもよい。ソフトウェアの暗号化の方法については各種の先行技術が知られておりここでは説明を省略する。ソフトウェアを暗号化する前にファイル圧縮プログラムなどで圧縮操作を行うことにより、CD-ROM120上の領域を節約できる。この圧縮操作も公知の技術なので説明は省略する。

【0016】パスワード解析プログラム140では、ユーザ20が入力したパスワード130を解析し、使用許諾されているソフトウェアのビット列210が生成される。このビット列を元にCD-ROM120に格納される暗号化ソフトウェア160を復号化処理プログラム150で復号化し、インストールを行うことによりユーザ20はソフトウェアを利用できるようになる。パスワード解析プログラム140での解析手順については図2で説明する。

【0017】パスワード生成システム100での、使用許諾するソフトウェアリストのビット列200から暗号

化処理300されバイナリデータ301となり、バイナリデータ301から文字列化処理302にて文字列変換テーブル303を用いてパスワード130が生成されるまでの過程については図3で説明する。

【0018】復号化処理プログラム150では、暗号化ソフトウェアの復号化処理を行う。パスワード解析プログラム140で得られた使用許諾されているソフトウェアのビット列210から復号化処理プログラム140の入力となる暗号化ソフトウェアを判別する。

【0019】図1の例では、ユーザ20はソフトウェアa、c、dを購入する場合の例を示している。パスワード解析プログラム140により得られたビット列210からCD-ROM120に格納してある暗号化ソフトウェア160のうちの暗号化ソフトウェアa160a、暗号化ソフトウェアc160c、暗号化ソフトウェアd160dを復号化処理プログラム150の入力とする。復号化処理プログラム150でそれぞれの暗号化プログラム160の復号化処理を行った後、ユーザ20のパーソナルコンピュータ170内にインストールを行いユーザ20が購入したソフトウェア180a、180c、180dのみを利用できる状態にする。

【0020】このように本発明では、一つのパスワード130で複数のソフトウェアのインストールを可能にすることにより、数十のソフトウェアを複数台のパーソナルコンピュータにインストールする大規模な企業ユーザなどの場合にはソフトウェアのインストール作業の労力を大幅に削減することができる。

【0021】次に図2を参照してパスワード130の生成から解析までの処理の流れを説明する。ユーザ20は購入したいソフトウェアをソフトウェア供給者10に対し注文すると、ソフトウェア供給者10はパスワード130を生成するために使用許諾するソフトウェアリストのビット列200を生成する。この使用許諾するソフトウェアリストのビット列200とCD-ROM120に関する情報やCD-ROM120に格納されているソフトウェアのソフトウェアリストに関する情報を元に、パスワード生成システム100ではこれらの情報に対し暗号化処理を行い、出力されデータを文字列に変換することによりパスワード130が生成される。

【0022】次に図3を参照してパスワード生成システム100内の処理である、使用許諾するソフトウェアリストのビット列200からパスワードが生成されるまでの流れを説明する。

【0023】使用許諾するソフトウェアリストのビット列200は暗号化処理300されるとバイナリデータ301が生成される。このバイナリデータ301をパスワード解析プログラム140内の復号化処理にかければ使用許諾されたソフトウェアリストのビット列201が得られCD-ROM120内のソフトウェアをインストールすることができるようになる。これを実現するために

バイナリデータ301をパスワード130として文字列に変換してユーザに提供しなければならない。

【0024】バイナリデータ301からパスワードに変換する処理部分を文字列化処理302と呼ぶことにする。文字列化処理302には文字列変換テーブル303がある。文字列変換テーブル303は全部で41文字で構成されていて、その内訳は0～9(1を除く)、a～z(i, lを除く)、記号(<=>*+-%)とする。文字列変換テーブル303を構成している文字がユーザに渡される文字となるので、印刷した場合など判別しにくい文字列は構成文字からはずした。例えば、1(イチ)とl(エル)とi(アイ)は判別しにくいため文字列変換テーブル303に入っていない。また、アルファベットの小文字のみを構成文字としたため0(ゼロ)とo(オウ)は判別できると判断し構成文字としている。

【0025】文字列変換処理302ではバイナリデータ301を2バイトずつ取り出し、文字列変換テーブル303を用いて3文字分のパスワード130を生成している。すべてのバイナリデータ301をパスワード130に変換するとパスワード生成システムでの処理は完了する。

【0026】ユーザ20はソフトウェア供給者10から受け取ったパスワード130をパーソナルコンピュータに入力すると、パスワード解析プログラム140が起動しパスワード130の解析が行われる。パスワード解析プログラム140では、入力されたパスワード130をバイナリデータ化し、そのデータを復号化処理することにより元のデータを取り出すことができる。取り出したデータのうち、使用許諾されているソフトウェアリストのビット列210はどの暗号化ソフトウェアを復号化処理するかを判別に使用する。その他のデータは、入力されたパスワード130の正否の判定に使用している。もし、ユーザ20が入力したパスワード130の正否の判定でエラーと判別した場合は、パスワード130が間違っていることを示すメッセージを表示しパスワード130の再入力を促すようにする。以上説明してきた実施例では配布される記憶媒体にCD-ROMを使用した。が、CD-ROMに限らず各種光磁気ディスク、将来採用されるであろうDVDや8ミリテープ、デジタルデー

タストリーマなどのテープメディアでもよい。

【0027】

【発明の効果】本発明は、以上説明したように構成されているので、大容量の配布媒体に複数の暗号化したソフトウェアを格納して配布してもユーザ20が購入したソフトウェアのみが利用できるようになり、購入していないソフトウェアの不正使用が防止でき、さらに、1つのパスワード130でユーザ20が購入した複数のソフトウェアを復号化し利用できるようになるので、複数のソフトウェアのインストール作業の煩雑さが大幅に軽減されるという効果がある。

【図面の簡単な説明】

【図1】本発明の一実施例を示すソフトウェアの配布方法を説明するための図である。

【図2】本発明で使用するパスワードの生成から解析までの流れを説明するための図である。

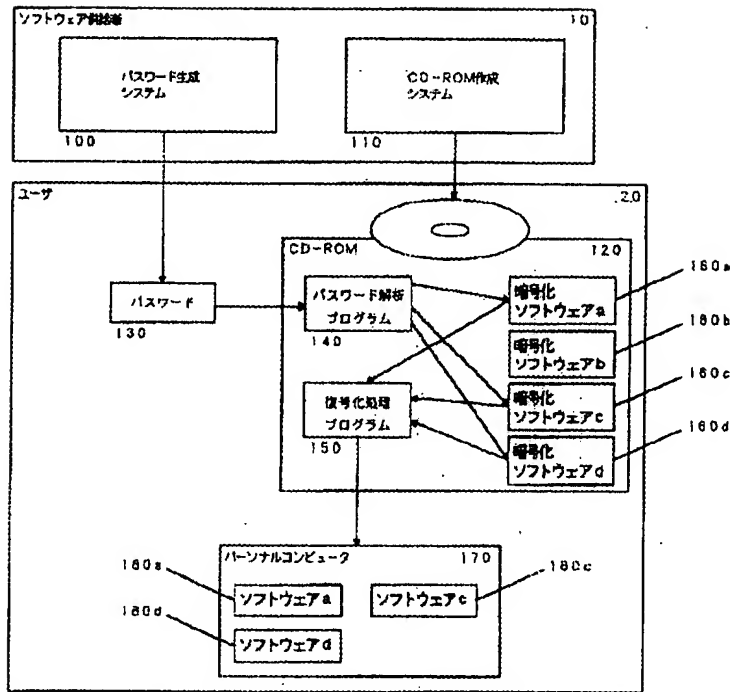
【図3】本発明で使用するパスワード生成システム内のパスワード生成処理の流れを説明するための図である。

【符号の説明】

- 10 ソフトウェア供給者(ソフトウェアベンダなど)
- 20 ユーザ
- 100 パスワード生成システム
- 110 CD-ROM作成システム
- 120 CD-ROM
- 130 パスワード
- 140 パスワード解析プログラム
- 150 復号化処理プログラム
- 160 暗号化ソフトウェア
- 170 パーソナルコンピュータ
- 180 ソフトウェア(ユーザが購入し復号化処理されている)
- 200 使用許諾するソフトウェアリストのビット列(ユーザが購入希望するソフトウェア)
- 210 使用許諾されたソフトウェアリストのビット列(ユーザが購入したソフトウェア)
- 300 暗号化処理
- 301 バイナリデータ
- 302 文字列化処理
- 303 文字列変換テーブル

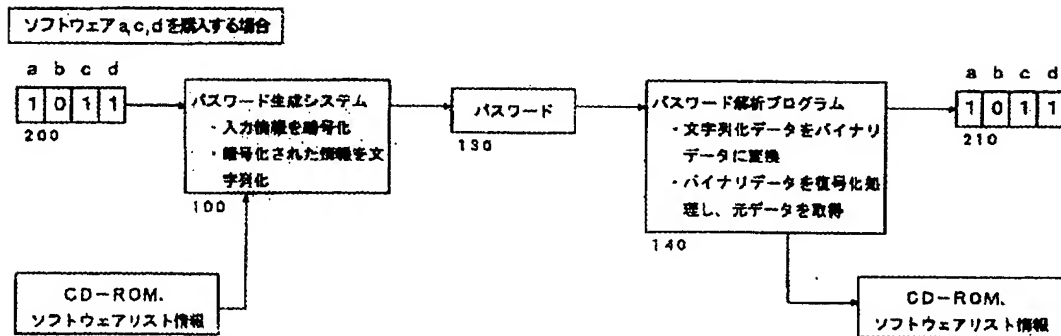
【図1】

図1



【図2】

図2



【図3】

図 3

